CLAIMS

What is claimed is:

1. A partially encrypted signal comprising:

a plurality of encrypted packets, a portion of said encrypted packets encrypted according to a first encryption scheme to define first encrypted packets and another portion of said encrypted packets encrypted according to a second encryption scheme to define second encrypted packets; and

a plurality of unencrypted packets, wherein at least a portion of said unencrypted packets, at least one of said first encrypted packets, and at least one of said second encrypted packets are indistinguishable from one another based upon a packet identifier, and wherein said at least one each of said first and second encrypted packets being indistinguishable from one another based upon said packet identifier are also indistinguishable based upon a continuity count.

2. The partially encrypted signal of Claim 1 received in a set-top, said set-top adapted to select either of said first and second encrypted packets, being indistinguishable from one another based upon said packet identifier and said continuity count, based upon the order said first and second encrypted packets are received relative to one another in said set-top.

3. The partially encrypted signal of Claim 2 wherein said selected one of said first and second encrypted packets is decrypted to produce decrypted content and the other said packet of said first and second encrypted packets is discarded.

4. The partially encrypted signal of Claim 1 wherein said first and second encrypted packets have duplicate content and are adjacent to one another in said signal, and wherein a continuity counter of said second encrypted packet has not been incremented.

5. The partially encrypted signal of Claim 1 wherein packet identifiers of said first and second encrypted packets have not been remapped.

6. A method of partially encrypting content comprising the steps of:

packetizing said content into a plurality of packets and at least a portion of said plurality of packets having an identical packet identifier;

reproducing a critical packet to produce duplicate packets having said identical packet identifier;

encrypting one of said duplicated packets according to a first encryption scheme to produce a first encrypted packet and encrypting the other of said duplicated packets according to a second encryption scheme to produce a second encrypted packet; and

distinguishing between said first and second encrypted packets having said identical packet identifier based upon the alignment of said first and second encrypted packets relative to one another.

7. The method of Claim 6 further comprising the steps of consecutively incrementing a continuity counter of each said plurality of packets having said identical packet identifier when packetizing said content, and maintaining said identical packet identifier and identical values for each said continuity counter of said duplicated packets.

8. A method of processing packets, comprising the steps of:

receiving first a first encrypted packet having a first packet identifier and a first continuity counter;

receiving second a second encrypted packet having said first packet identifier and said first continuity counter, wherein said first and second encrypted packets were encrypted according to first and second encryption schemes, respectively;

distinguishing between said first and second encrypted packets based upon the order said first and second encrypted packets are received; and

performing one of the following steps:

discarding said first encrypted packet because said second encrypted packet was received subsequent to receiving said first encrypted packet; or

discarding said second encrypted packet because said first encrypted packet was received before receiving said second encrypted packet.

9. The method of Claim 8 further comprising the steps of decrypting and decoding one of the first and second encrypted packets which has not been discarded.

10. A method of decoding partially encrypted content comprising the steps of:

receiving partially encrypted content comprising unencrypted content, first encrypted content encrypted under a first encryption scheme and second encrypted content encrypted under a second encryption scheme;

selecting one of said first and second encrypted content to decrypt based upon the alignment of said first and second encrypted content relative to one another;

decrypting said selected one of said first and second encrypted content to produce decrypted content; and

decoding said unencrypted content and said decrypted content to decode said partially encrypted content.

11. The method of Claim 10 wherein said first and second encrypted content is packetized into packets and at least a portion of said packets of said first and second encrypted content is received having the same packet identifier.

12. The method of Claim 10 wherein said first and second encrypted content is packetized into packets and at least a portion of said packets are received having the same value for a counter incremented to verify continuity of said packets.

13. A television set-top box comprising:

a receiver that receives:

a plurality of unencrypted packets;

a plurality of first encrypted packets encrypted according to a first encryption scheme; and

a plurality of second encrypted packets encrypted according to a second encryption scheme; and

a decrypter that discards one of said first and second encrypted packets based upon the alignment of said first and second encrypted packets relative to one another and decrypts the other of said first and second encrypted packets.

14. The television set-top box of Claim 13 wherein one of said second encrypted packets is received subsequent to one of said first encrypted packets, said one second encrypted packet is decrypted, and said one first encrypted packet is discarded.

15. The television set-top box of Claim 13 wherein at least one of said first encrypted packets and at least one second encrypted packets are indistinguishable from one another based upon a packet identifier.

16. The television set-top box of Claim 13 wherein at least one of said first encrypted packets and at least one of second encrypted packets are indistinguishable from one another based upon a continuity count.

17. The television set-top box of Claim 13 wherein at least a portion of said unencrypted packets, at least a portion of said first encrypted packets, and at least a portion of said second encrypted packets have an identical packet identifier.

18. The television set-top box of Claim 13 wherein at least a portion of said unencrypted packets, at least a portion of said first encrypted packets, and at least a portion of said second encrypted packets have an identical packet identifier, and wherein said at least a portion of said first encrypted packets and at least a portion of said second encrypted packets have an identical continuity counter.

19. A method of managing multiple access control systems utilizing partially encrypting content, said method comprising:

reproducing a critical packet from packetized content to produce duplicate packets;

encrypting one of said duplicate packets according to a first encryption scheme to produce a first encrypted packet;

encrypting the other of said duplicate packets according to a second encryption scheme to produce a second encrypted packet;

transmitting said first and second encrypted packets along with unencrypted packets of said packetized content to at least one of said multiple control access systems; and

decrypting one of said first and second encrypted packets based upon the alignment of said first and second packets relative to one another.

20. The method of Claim 19 further comprising the step of utilizing an identical packet identifier for said first and second encrypted packets.

21. The method of Claim 19 further comprising the step of maintaining an identical packet identifier for said duplicated packets in order to perform said encryption steps.

22. The method of Claim 19 further comprising the steps of associating at least a portion of said plurality of packets of said packetized content with one another with a counter and consecutively incrementing said counter to designate said at least a portion of said plurality of packets as being continuous, and utilizing an identical value for said counter after reproducing said critical packet and after separately encrypting both said duplicate packets.

23. The method of Claim 22 wherein said decrypting step comprises decrypting said first encrypted packet because said first encrypted packet was received before said second encrypted packet.

24. The method of Claim 22 wherein said decrypting step comprises decrypting said second encrypted packet because said second encrypted packet was received after said first encrypted packet.

25. The method of Claim 19 wherein said decrypting step of said one of said first and second encrypted packets is performed by identifying said first and second encrypted packets having an identical continuity counter as a result of an unincremented continuity counter of either of said first and second encrypted packets and is further performed by decrypting said one of said first and second encrypted packets received subsequent to the receipt of the other of said first and second encrypted packets.

26. The method of Claim 19 further comprising at least one of the following steps:

discarding said first encrypted packet because said second encrypted packet was received subsequent to receiving said first encrypted packet; or

discarding said second encrypted packet because said first encrypted packet was received before receiving said second encrypted packet.

27. The method of Claim 19 wherein identical packet identifiers of said duplicated packets and identical continuity counts of said first and second encrypted packets are maintained throughout said method.

28. The method of Claim 19 wherein said step of transmitting said first and second encrypted packets comprises forgoing incrementing a continuity counter of one of

said first and second encrypted packets to be transmitted subsequent to the other of said first and second encrypted packets.

29. The method of Claim 19 performed without remapping a packet identifier of said duplicate packets.

30. The method of Claim 19 free from remapping packet identifiers to distinguish between said first and second encrypted packets.